International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 3, March - 2013

An Innovative Watermarking Scheme For Digital Image Authentication With Common Image Processing

[A]Mrs. Dhanashri D. Dhokate.
P. V. P. I. T. Budhgaon.
Sangli, India

[B]Dr. Vijay R. Ghorpade
D. Y. P C. O. E
Kolhapur, India

Abstract

The central idea of this paper is to propose an innovative watermarking scheme for digital image authentication which withstands common image processing attacks. The digital revolution in digital image processing has made it possible to create, manipulate and transmit digital images in a simple and fast manner. The adverse affect of this is that the same image processing techniques can be used by hackers to tamper with any image and use it illegally. This has made digital image safety and integrity the top prioritized issue in today's information explosion. Watermarking is a popular technique that is used for copyright protection and authentication.

This paper presents an overview of the various concepts and research works in the field of image watermark authentication. In particular, the concept of content-based image watermarking is reviewed in details. Some pixels are randomly selected from original image, so that all of them have valid 3 × 3 neighborhoods. A binary sequence is constructed from those pixels by comparing them against average values of neighborhoods. The binary sequence is then converted into a watermark pattern in the form of a Hankel matrix to improve security of watermarking process and is then embedded within the host image.

The operation of embedding and extraction of watermark is done in high frequency domain of Discrete Wavelet Transform since small modifications in this domain are not perceived by human eyes. This watermarking scheme deals with the extraction of the watermark information in the absence of original image, hence the blind scheme was obtained.

1. Introduction

The internet is an excellent distribution system for the digital media because of its inexpensiveness and efficiency. Also the images can be readily shared, easily used, pro-cessed and transmitted which causes serious problems such as unauthorized use and manipulation of digital con-tent. As a result, there is the need for authentication techniques to secure digital images. Digital watermarking is a technique which embeds additional information called digital signature or watermark into the digital content in order to secure it. A watermark is a hidden signal added to images that can be detected or extracted later to make some affirmation about the host image. The major point of digital watermarking is to find the balance among the aspects such as robustness to various attacks, security and invisibility. The invisibleness of watermarking technique is based on the intensity of embedding watermark. Better invisibleness is achieved for less intensity watermark. So we must select the optimum intensity to embed watermark. In general there is a little trade o® between the embedding strength (the watermark robustness) and quality (the watermark invisibility). In-creased robustness requires a stronger embedding, which in turn increases the visual degradation of the images. For a watermark to be effective, it should satisfy the following features. They are:

1. **Imperceptibility** - It should be perceptually invisible so that data quality is not degraded and attackers
are prevented from finding and deleting it.
2. **Readily Extractable** - The data owner or an independent control authority should easily extract it.
3. **Unambiguous** - The watermark retrieval should un-ambiguously identify the data owner.
4. **Robustness** - It should tolerate some of the common image processing attacks.

The commonly used watermarking applications include copyright protection, authentication, and ownership identification. The digital image watermarking scheme can be divided into two categories. They are visible digital image

watermarking and invisible image watermarking techniques. Furthermore the invisible watermarks are categorized into watermarking techniques as fragile and robust.
Generally, a robust mark is designed to resist attacks that attempt to remove or destroy the mark. These algorithms ensure that the image processing operations do not erase.

2. Proposed Watermarking Scheme

The wavelet decomposition decomposes the image into three spatial directions i.e. horizontal, vertical and diagonal. Hence wavelets reflect the anisotropic properties of HVS more precisely. The human visual system (HVS) is related to the perceptual quality [2], measured according to the sensitivity/sharpness of a human eye to see details in an image. Research into human perception indicates that the retina of the eye splits an image into several frequency channels each spanning a bandwidth of approximately one octave. The signals in these channels are processed independently. Similarly, in multi resolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process of imperceptible watermarking more effective [3]. The multi resolution successive approximation not only enhances the resolution of an image, but also enhances the resolution of watermark simultaneously. This advantage of the DWT allows using higher energy watermarks in regions where the HVS is known to be less sensitive so that embedding watermarks in these regions provides to increase the robustness of the watermarking techniques.

In this paper, a meaningful image watermark is embedded in the DWT domain. The watermark detection is a blind method i.e. is without the use of original image [4]. We embed a watermark into an image by modifying coefficients of mid frequency bands i.e. LH and HL subbands, and extract the watermark by analyzing perturbation of coefficients from a suspected image.

2.1 Discrete Wavelet Transform (DWT)

The Fourier transform, which provides a representation of the transformed signal in the frequency domain, is widely used in signal processing. However, the loss of time information in a signal by Fourier transform will leads to the difficulty in processing [8]. The wavelet transform is an excellent time-frequency analysis method, which can be well adapted for extracting the information content of the image.

2.2 Multiple-Level Decomposition:

Applying a 1-D wavelet transform to all the rows of the Image and then repeating on all of the columns can compute the 2-D wavelet transform. When one-level 2-D DWT is applied to an Image, four transform coefficient sets are created.

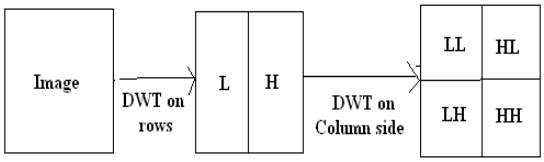


Fig.1 DWT Decomposition of image

The four sets are LL, HL, LH, and HH, where the first letter corresponds to applying either a low pass frequency operation or high pass frequency operation to the rows, and the second letter refers to the filter applied to the columns Which is shown in Fig.1 .

Fig.1 DWT Decomposition of image wavelet analysis of an original image can be divided into an approximate image LL and three details images LH, HL and HH., the approximate image hold most of the information of the original image, while the others contain some details such as the edge and textures will be represented by large coefficients in the high frequency sub-bands [15]. The reconstruction of the image is achieved by the inverse discrete wavelet transform (IDWT).

2.3 Spread spectrum Watermarking

To overcome the limitations in watermarking due to methods like LSB (least significant bit) substitution and to make the system more robust against attacks, the watermark can be spread across the cover object by using more number of bits than the minimum required. This scheme of hiding the data ensures the survival of watermark under various attacks due to redundancy. Generally the message used to watermark is a narrow band signal compared to the wide band of the original image. Spread spectrum techniques [5] applied to the message allows the frequency bands to be matched before embedding the watermark through the original

image. Spread spectrum technique also offer the possibility of protecting the watermark privacy using a secrete key to control a pseudo noise generator.

For a one level decomposition, the discrete two-dimensional wavelet transform of the image function f (x, y) can be written as [5].

$$LL = [(f(x, y) * \Phi(-x)\,\Phi(-y)(2n,2m))](n, m) \in Z^2$$

$$LH = [(f(x, y) * \Phi(-x)\,\psi(-y)(2n,2m))](n, m) \in Z^2$$

$$HL = [(f(x, y) * \psi(-x)\,\Phi(-y)(2n,2m))](n, m) \in Z^2$$

$$HH = [(f(x, y) * \psi(-x)\,\psi(-y)(2n,2m))](n, m) \in Z^2$$

Where $\Phi(t)$ is a low pass scaling function and $\psi(t)$ is the associated band pass wavelet function.

3. Proposed Method

In the proposed scheme, there are three significant phases: Watermark generation, Watermark embedding and Watermark Detection. The watermark is generated from pixel value of original image and so there is no need of external image or logo. Hence it is necessary to devise a method to generate watermark. The resolution of water-mark is assumed to be half of the original image. For embedding the watermark, a 1-level Discrete Wavelet Transform is performed. Watermark information is embedded in the high frequency bands (HH1) since it is robust against various normal image processing and malicious attacks. The resultant image is called watermarked image. In detection phase, watermark is once again generated from watermarked image and also extracted the embedded watermark from HH1 sub band. Comparison is made between those watermarks to decide authenticity.

3.1 Watermark Generation

The watermark pattern is generated from the spatial do-main information. Watermark generation procedure includes the following steps:

- Consider the original image P of size M X M.
- Perform 1-level DWT on the original image and ac-quire the LL1 component to find watermark pattern, which is of size M/2 X M/2. Let this matrix be `A'.
- A reduced size (M/2 X M/2) image `B' is obtained from original image by performing the following steps-

- Partition the original image into non-overlapping blocks of size 2X2.

- Compute one feature value from each block ac-cording to the following equation.

$$B(x, y) = \frac{\sum_{i=1}^{2}\sum_{j=1}^{2} P(x*2 + i, y*2+j)}{4}$$

Where, $0 <= x <= M/2$ and $0 <= y <= M/2$

Find the difference between A and B. Let it be C.

- A binary sequence `W ' can be obtained by applying the following constraint

$$W(x, y) = \begin{cases} 0; & \text{if } C(x, y) \text{ is even} \\ 1; & \text{otherwise.} \end{cases}$$

- Disorder the matrix `W ' with the help of Arnold Transform, which is the required watermark pattern to be embedded within the host image.

3.2 Watermark Embedding Technique

The pseudorandom sequences generated with the key as the initial seed is added [1] to the horizontal and vertical DWT coefficients (HL, LH) of the original image according to the equation :-

$$\mathbf{Iw(x, y) = I(x, y) + k \times W(x, y)}$$

In which I(x,y) representing the DWT coefficients of the original image, Iw (x, y)) is the watermarked image, K denotes the gain factor that is usually used to adjust the invisibility of the watermark.

The robustness of the watermarked image increases as the gain K increases. But, with increase in the gain Kthe quality of the final watermarked image reduces. If the pixel in the watermark vector is zero then the PN sequence with appropriate gain is added to the selected Subband coefficients, the watermark embedding process is shown in Fig.2

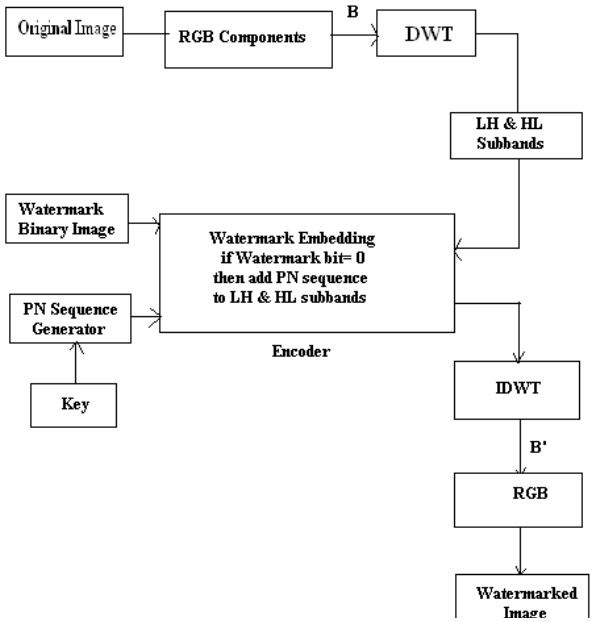
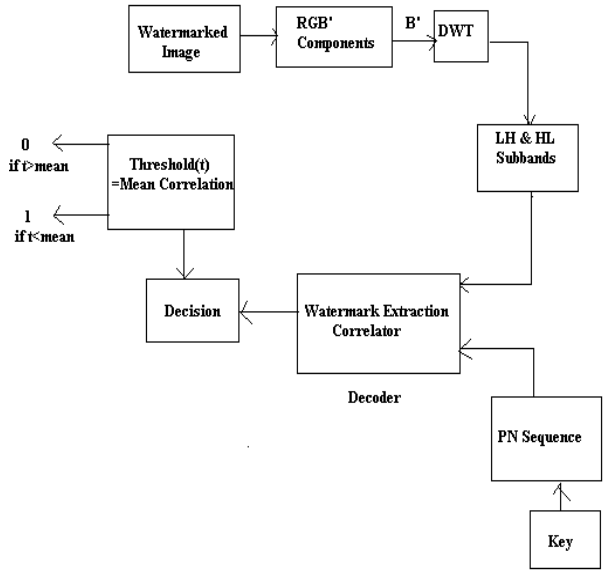


Fig 2. Watermark embedding process

4. Watermark Extraction Technique

Proposed watermarking scheme deals with the extraction of the watermark information in the absence of the original image, i.e., blind watermarking. Hence correlation measure [5] is used to detect the watermark. The correlation is calculated between the generated PN sequence matrix and modified sub band coefficients for each of the pixels in the watermark string and if it exceeds a particular threshold then the watermark is said to be detected. The threshold for the decision is set as the mean of the correlation value for all the pixels. During computation in the first level resolution the watermark is called detected, if the correlation between the extracted bits and the original bits is above a threshold.

If there is no watermarked detected then, the decoder adds the second resolution level. Once again, if the correlation between the extracted bits and the original bits is above a threshold then the watermark is detected. The watermark extraction process is shown in Fig.3



.Fig. 3 Extraction process

5. Performance Evaluation of Proposed Watermarking Scheme:

Watermark is embedding in the original image bird. The watermarked and difference Images are shown in Fig 4, is the absolute difference of the pixel intensities of the watermarked image and the original image. The difference image gives the visual modifications of the coefficients. Results shown in Figure 4: with selected gain.

Fig.4. Watermarked image and Difference image Watermarked Image and the extracted watermark for the gain of 0.6 and at level II deco potion is shown in Fig 5.

Watermarked Image Difference Image

Fig.4 Watermarked image and difference

Fig: 5 Watermarked Image and Extracted watermark The simulation results

shows that the PSNR value is high around 46.85 for level II decomposition it is 41.61 for level I decomposition.

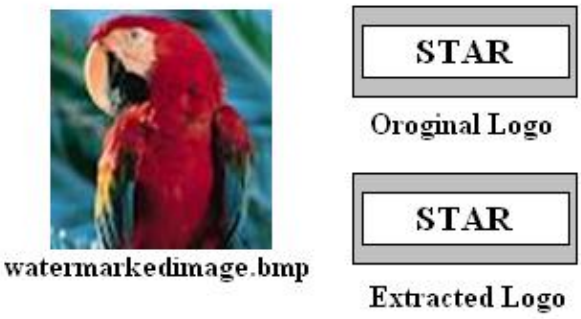


Fig.5 Watermarked image and extracted watermark

6. Conclusion

This study has proposed a robust watermarking which provides a complete algorithm that embeds and extracts the watermark information effectively. In this method, a watermark pattern is constructed from host image itself. Watermark signal is disordered with the help of Arnold Transform. The designed method makes use of the low frequency component of Discrete Wavelet Transform for watermarking construction process and high frequency component for the embedding and extraction processes.

Moreover the authentication process provides qualities like imperceptibility, robustness and security. The performance of the watermarking scheme is evaluated with common image processing attacks such as adding noises, filtering, intensity adjustment, histogram equalization, JPEG compression, Scaling and rotation.

Experimental results demonstrate that watermark is robust against those attacks. Moreover the simulation results of currently devised method are compared with that of our previous work, the results obtained show that the proposed technique is highly robust against attacks such as JPEG compression, scaling and rotation.

7. References

[1]A Study on Watermarking Schemes for Image Authentication www.ijcaonline.org/archives/volume2/number4/658-925.
[2] Peter Meerwald, " Digital image watermarking in the wavelet Transform domain " P.Hd thesiss.
[3] Houng- Jyh Mike Wang, Po-Chyi Su and C.-C. Jay Kuo, "Wavelet-based digital image watermarking" OPTICS EXPRESS, 7 December 1998 / Vol. 3, No. 12,PP 491-496 .
[4] [1] Arvind Kumar Parthasarathy and Subhash Kak "An Improved Method of Content Based Image Watermarking "IEEE Transaction on broadcasting, Vol.53, No. 2, June 2007, PP 468
[5] S. Kumar, B. Raman, and M. Thakur, \Real coded genetic algorithm based stereo image watermarking," JSDIA, vol. 1, no. 1, pp. 23-33, 2009.
[6]M. Kuttera and F. A. P. Petitcolas, " A fair benchmark for image watermarking systems"

Mrs. Dhanashri D. Dhokate was born in Sangli, 24th Dec. 1982. She has completed Diploma in Comp. Engg,(ICRE, Gargoti, India, March-2000) from Mumbai universiry, BE CSE(Walchand college of Engg, Sangli, Maharashtra, India ,March 2005)from Shivaji University and appeared for ME CSE at D. Y. Patil College of Engg,Shivaji university.

She has teaching experience of 7 years and working as an ASSISTANT PROFESSOR in PVPIT, Budhgaon, and Sangli, India. Her 5 papers are selected and registered in different international conferences out of those 2 are explored by IEEE Explorer. She has published 2 paper in international journal.

Vijay Ram Ghorpade, was born in Maharashtra, India, on July 20, 1968. He received the B.E. degree and M.E. degrees in Computer Science and Engineering from Marathwada University, Aurangabad, and Shivaji University, Kolhapur, India, in 1990 and 2001 respectively. In 2008, he earned his PhD degree at SGGSIET, Nanded, India. Presently he is working as Principal at D. Y. Patil College of Engineering and Technology, Kolhapur, India. His research interests include network security and ad hoc networks.